

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

(12) UK Patent Application (19) GB (11) 2 369 530 (13) A

(43) Date of A Publication 29.05.2002

(21) Application No 0028618.7

(22) Date of Filing 24.11.2000

(71) Applicant(s)
Telefonaktiebolaget LM Ericsson
(Incorporated in Sweden)
S-126 25 Stockholm, Sweden

(72) Inventor(s)
Esa Turtiainen
Jari Arkko
Pasi Ahonen

(74) Agent and/or Address for Service
Marks & Clerk
4220 Nash Court, Oxford Business Park South,
OXFORD, OX4 2RU, United Kingdom

(51) INT CL⁷
H04Q 7/38

(52) UK CL (Edition T)
H4L LRCMA L205 L207

(56) Documents Cited
GB 2342817 A WO 01/17310 A1
WO 00/02406 A2

(58) Field of Search
UK CL (Edition S) H4L LDPD LDPPX LRCMA LRCMS,
H4P PDCSA
INT CL⁷ H04L 9/32 29/06, H04Q 7/38
ONLINE: WPI, EPODOC, JAPIO, INSPEC

(54) Abstract Title
IP security connections for wireless authentication

(57) A mobile, 4, is authenticated and identified by a gateway node, 8, which produces and sends a certificate to the correspondent node, 2. The correspondent node uses the certificate to authenticate the gateway and identify the mobile. The system may be used to provide access for IP traffic to an intranet. The first leg of the authentication may use SIM, IKE, public private keys, SSL or TLS. The second leg may use a token to provide authority to allow access, and use a certification authority (CA.) The gateway node may be an operator owned security gateway. The certificate may contain information about the identity of the mobile, such as the phone number. The mobile may be any laptop, palmtop computer or PDA with cellular capabilities.

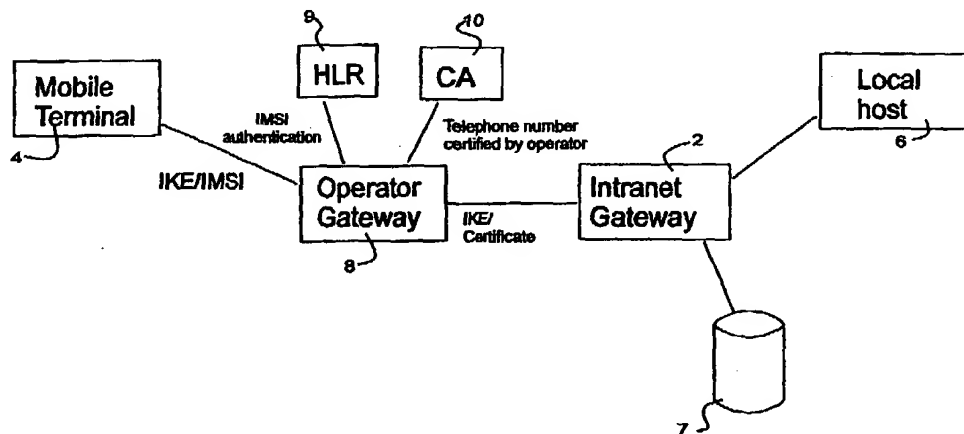


Figure 2

GB 2 369 530 A

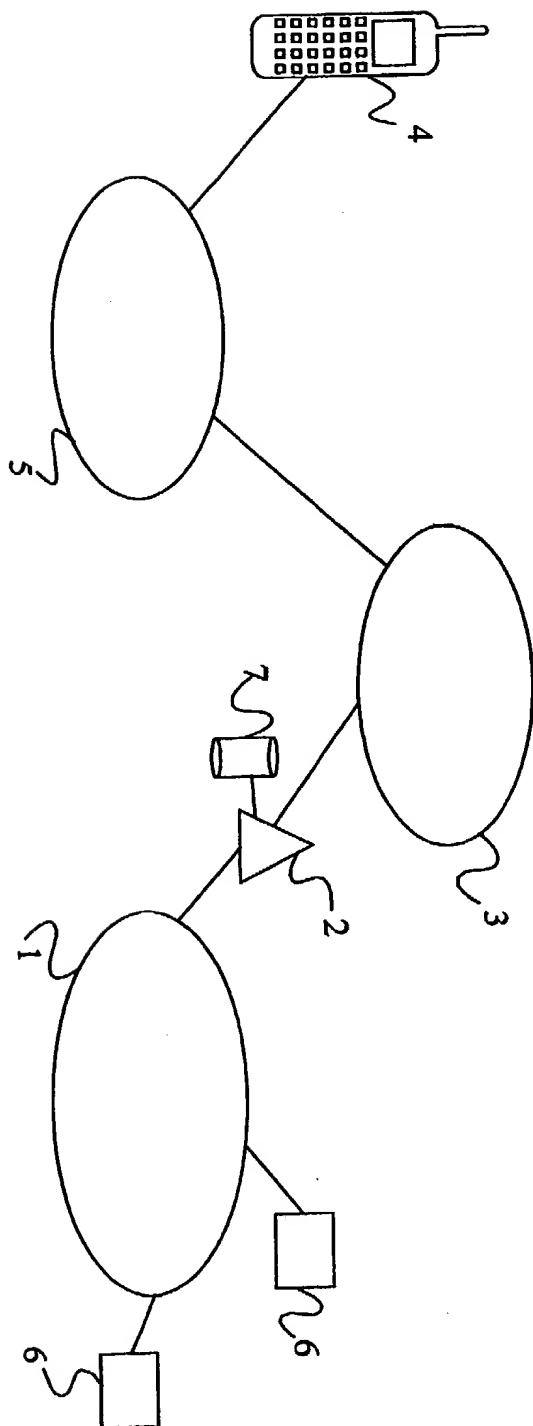


Figure 1

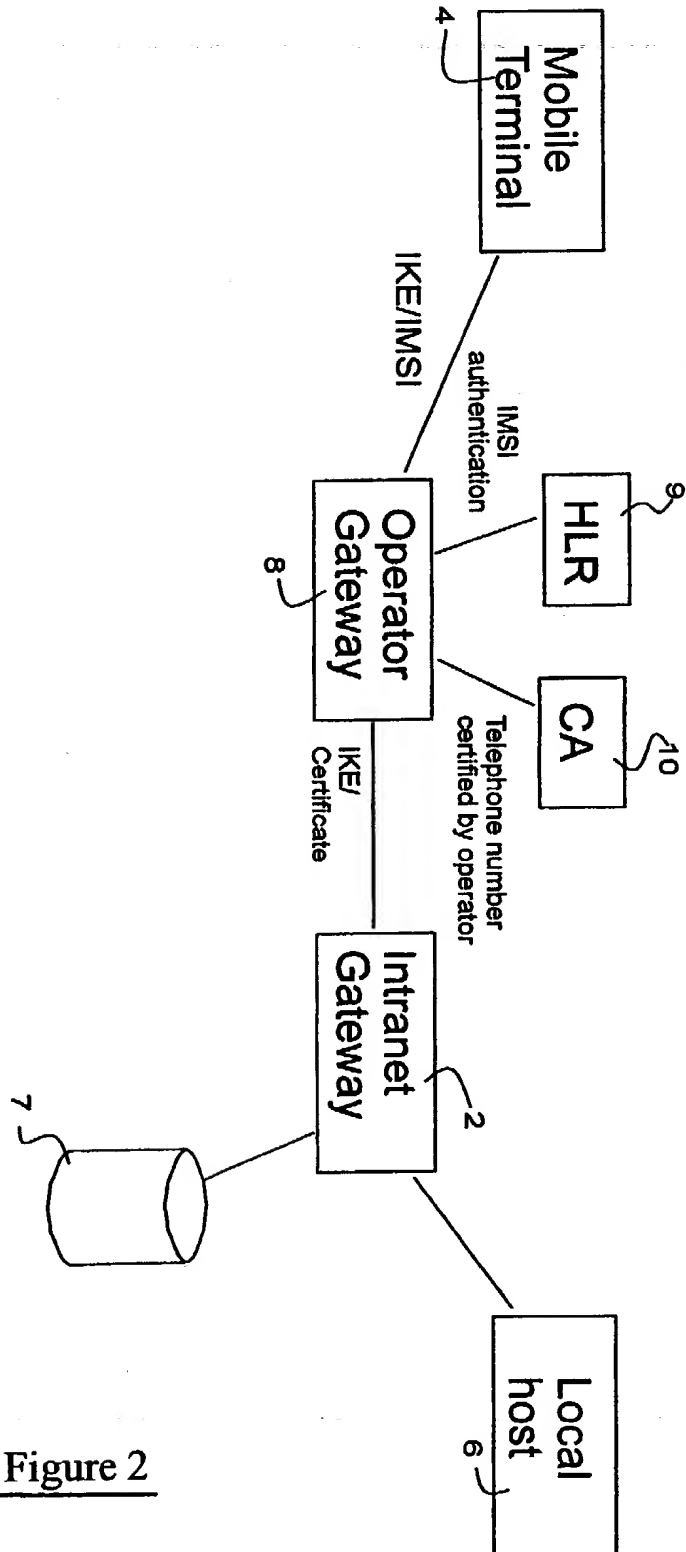


Figure 2

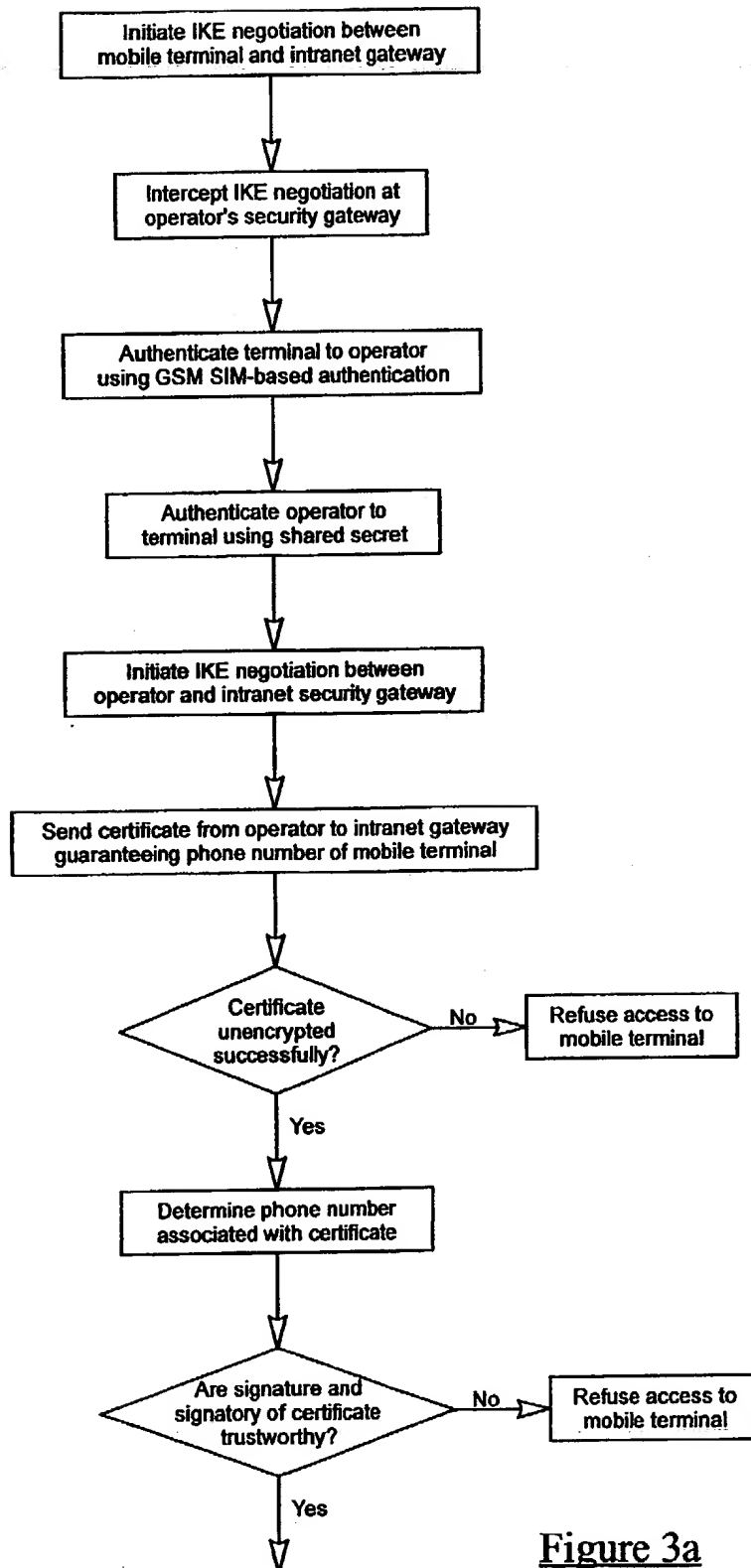


Figure 3a

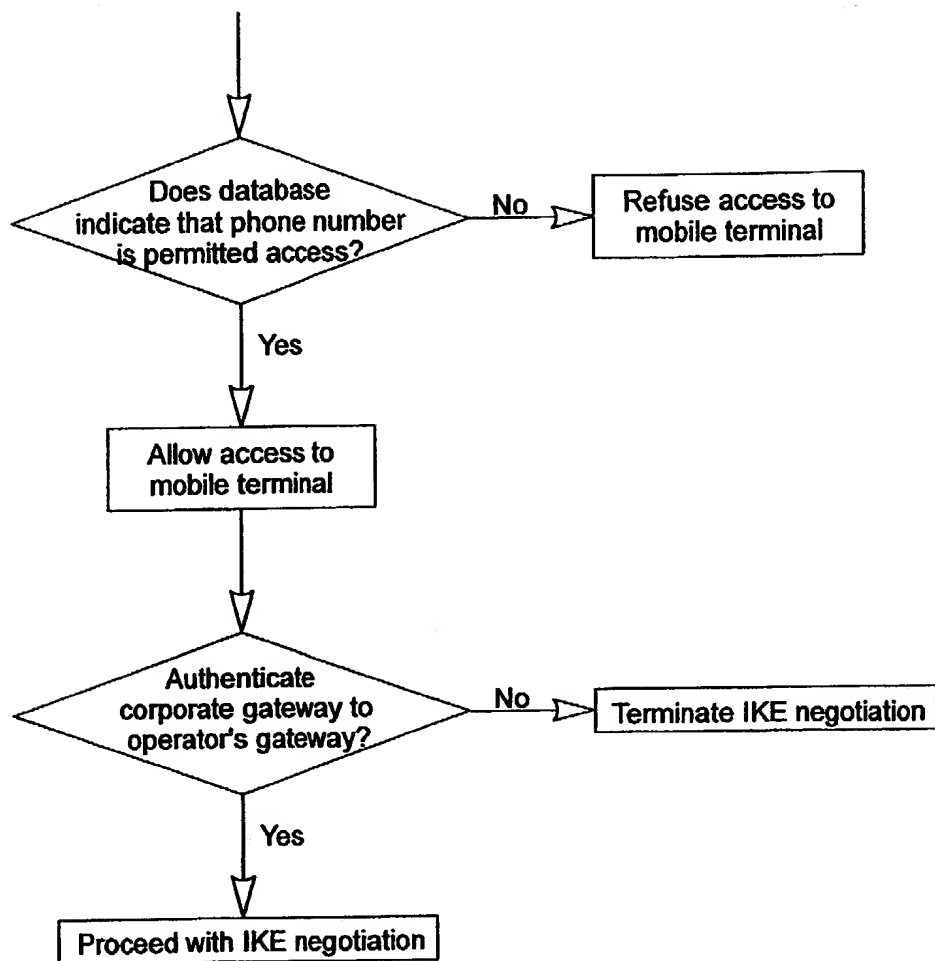


Figure 3b

IPSEC CONNECTIONS FOR MOBILE WIRELESS TERMINALS

The present invention is related to the optimisation of IPsec data transfer mechanisms for mobile wireless terminals and more particularly to the optimisation of IPsec authentication procedures.

Background to the Invention

IP connections between mobile wireless terminals (such as mobile telephones, communicators, and PDAs with wireless communication facilities) and entities such as corporate intranets are becoming increasingly popular. However, an organisation maintaining an intranet may wish to restrict access to selected users and to ensure that all data transfer between the intranet and those users is securely encrypted. IPsec (Internet Protocol Security) is a set of protocols which has been defined by the Internet Engineering Task Force (RFC2401) to provide a security mechanism for IP and certain upper layer protocols such as UDP and TCP. IPsec protects IP packets and upper layer protocols during transmission between peer nodes by introducing proof of origin (i.e. authentication) and encryption. IPsec allows the creation of so-called Virtual Private Networks (VPNs).

In order to allow IPsec packets to be properly encapsulated and decapsulated it is necessary to associate security services (and parameters) between the traffic being transmitted and the remote node which is the intended recipient of the traffic. The construct used for this purpose is a "Security Association" (SA). SAs are negotiated between peer nodes using a mechanism known as "Internet Key Exchange" (IKE), and are allocated an identification known as a "Security Parameter Index" (SPI). The appropriate SA is identified to the receiving node by including the corresponding SPI in the IPsec header. Details of the existing SAs and the respective SPIs are maintained in a Security Association Database (SAD) which is associated with each IPsec node.

The security of the process depends crucially on the security of the initial identification of the nodes involved. A corporate intranet gateway needs to be sure that a mobile terminal initiating IKE is authorised to do so. IKE includes within it a mechanism to

perform such authentication, as do other known mechanisms such as SSL and TLS. All of these mechanisms are based on public key cryptography and rely on the guarantee of a trusted (typically independent) Certification Authority (CA) that a particular user is associated with a particular key. Each node must obtain a public-private key pair.

5 Messages encoded with a node's private key can only be decoded with the corresponding public key, and those encoded with the public key can only be decoded with the private key. Thus if a node sends a message encoded with the private key, the recipient can authenticate the message as coming from that node if he can decode the message using the public key and if he can be sure that the public key is associated with

10 that node. The CA's task is to ensure that the association between public keys and nodes can be trusted.

This is achieved by the CA issuing certificates to the nodes at the same time as they obtain their initial public-private key pair. The certificate for a particular node may

15 include the public key of that node together with the identity of the node. The certificate is itself "signed" by encrypting it with the private key of the CA. Thus another node receiving this certificate can be sure it was "signed" by the CA if it can be unencrypted using the public key of the CA. He can then also be sure of the association between the first node and its public key. Using such guarantees, connections can be

20 opened in a scalable way since not everybody needs to know everybody else beforehand: it is only necessary to know the public key of the CA.

These mechanisms can theoretically be used by mobile terminals. In practice, however, their deployment is difficult for a number of reasons.

25 Firstly, in order to participate in the authentication process of IKE, SSL, or TLS, a terminal needs a public-private key pair, as described above. The generation of this key pair requires a large amount of computational power, together with sophisticated software and preferably also a means for generating random numbers. Mobile terminals

30 frequently do not have sufficient resources to cope with these demands.

Furthermore, the terminal needs to obtain a certificate from a CA guaranteeing the association of the key pair, the user, and the CA. In order to do this, the user must

provide identification information (and may even have to attend the CA in person, e.g. to present his or her passport), and must operate complex software on the terminal to correspond with the CA server over the Internet. In some cases, it is even necessary to copy and paste text between the terminal's user interface and an Internet server. These
5 are complicated tasks on an ordinary mobile terminal, especially for inexperienced users. Again, the problem also arises that the terminal must have sufficient resources to run the complex software, and this is frequently not the case.

One method which has been proposed to circumvent this problem is to combine the IP
10 level authentication performed using the IKE protocol with the existing and computationally simple Global System for Mobile communications (GSM) SIM authentication (SIM authentication is normally carried out for subscribers of mobile telecommunication (GSM) networks upon registration of a subscriber with a network). The proposal is made in the IETF draft titled "GSM SIM Authentication Mode for IKE"
15 submitted by J. Rinnemaa of Nokia Oy, and involves wrapping certain SIM authentication information in ISAKMP messages of IKE. This avoids the need for a) RSA operations, b) certificate generation, c) initial key generation, and d) initial certificate enrolment, although it remains necessary to perform Diffie-Hellman and the remaining IKE tasks. Using this mechanism, IP connections can be initialised without
20 excessive computational load and there is no significant additional configuration or set-up burden on the terminal users.

The problem with this approach is that, if a connection is required between the mobile wireless terminal and a security gateway of say a corporate intranet, in order to perform
25 the SIM authentication the gateway requires access to authentication triplets from the GSM network. These authentication triplets must be obtained by the security gateway from the Home Location Register (HLR) or Authentication Centre (AUC) node of the GSM network. It is however unlikely that operators would be willing to divulge this information to third parties as it can be used for fraudulent purposes such as cell phone
30 cloning. This approach can in practice only be used where the security gateway is owned by the operator of the mobile network and does not solve the problem of the authentication of a mobile terminal wishing to connect to a security gateway outside the control of the network operator.

Statement of the Invention

The inventors of the present invention have realised that many mobile terminals do not have sufficient resources to use standard authentication methods for IP traffic. Furthermore, it is unlikely that mobile terminals will be permitted to use SIM based authentication procedures with entities other than the mobile network's own nodes.

It is an object of the present invention to overcome or at least mitigate the disadvantages noted in the preceding paragraphs. This and other objects are achieved at least in part by providing a two-leg authentication procedure from the mobile terminal to a correspondent node. The first leg is an authentication between the mobile terminal and an operator-owned gateway, in which the mobile terminal is authenticated to the gateway using a mechanism such as SIM authentication. The second leg is an onward authentication between the operator-owned gateway and the correspondent node, with the operator-owned gateway authenticating the mobile terminal to the correspondent node.

According to a first aspect of the present invention there is provided a method of authenticating a mobile wireless terminal to a correspondent node for the purpose of establishing an IP connection between the terminal and the node, the method comprising:

- authenticating and identifying the mobile terminal to a gateway node of a mobile telecommunications network;

- at the gateway node, obtaining a certificate for the mobile terminal, which certificate can be used to identify and authenticate the mobile terminal;

- sending the certificate from the gateway node to the correspondent node; and

- at the correspondent node, using the received certificate to identify and authenticate the mobile terminal.

Embodiments of the invention do not require that the mobile terminal authenticate itself directly to the correspondent node. Rather, the correspondent node trusts the gateway node to authenticate the mobile terminal. In particular, the correspondent node trusts

the gateway node to maintain the security of the mapping between the mobile terminal's identity and the determined certificate.

5 The gateway node is preferably an operator-owned security gateway, and this operator gateway preferably determines a public-private key pair on behalf of the mobile terminal, together with the certificate for the mobile terminal based on a mapping of a unique identifier (such as the E.164 address or IMSI) of the terminal.

10 Preferably, the certificate identified by the gateway is a public key certificate obtained from a certification authority (CA). The certificate contains *inter alia* an identifier of the mobile terminal, e.g. the telephone number. Assuming that the mobile terminal is authenticated to the correspondent node, the correspondent node preferably determines whether or not to authorise access to the mobile terminal on the basis of said identifier.

15 Preferably, said steps of sending the certificate from the gateway node to the correspondent node and of using the received certificate to authenticate the mobile terminal both form part of an IKE Phase 1 procedure. Similarly, the step of authenticating the mobile terminal to the gateway node forms part of a separate IKE Phase 1 procedure. However, this procedure makes use of the SIM authentication
20 procedure using the subscriber's IMSI. More particularly, SIM authentication data is wrapped inside ISAKMP messages of the IKE Phase 1 procedure.

The method of the first aspect of the invention may be carried out following the initiation of an connection by the mobile wireless terminal or by the correspondent
25 node. The order in which the steps of the method are carried out need not follow the listed order.

In a preferred embodiment, the mobile terminal attempts to perform IKE with the correspondent node, and this attempt is recognised by the operator gateway, causing the
30 operator gateway to authenticate the mobile terminal to the correspondent node and handle IKE negotiations with the correspondent node on behalf of the mobile terminal. Alternatively, the mobile terminal may contact the operator directly (for example, in response to information contained on a SIM card in the terminal or in response to the

user's configuration of the terminal) to cause the operator to open IKE negotiations with the second network node.

Preferably, the mobile wireless terminal is a cellular telephone or communicator, or a
5 PDA, laptop computer, palmtop computer etc, having cellular telephone capabilities.

According to a second aspect of the present invention there is provided a gateway node of a mobile telecommunications network, the gateway node comprising:

- means for authenticating and identifying a mobile wireless terminal;
- 10 means for obtaining a certificate for the mobile terminal, which certificate can be used to identify and authenticate the mobile terminal; and
- means for sending the certificate from the gateway node to the correspondent node,
- wherein the received certificate may be used by the correspondent node to
- 15 identify and authenticate the mobile terminal for the purpose of establishing an IP connection between the terminal and the node.

Brief Description of the Drawings

20 Figure 1 illustrates schematically a communications system incorporating a corporate intranet, the Internet, and a Public Land Mobile Network (PLMN);

Figure 2 illustrates schematically the nodes involved in authenticating a mobile terminal to a corporate intranet gateway across the system of Figure 1; and

25 Figures 3a and 3b show a flow diagram showing the steps involved in authenticating a mobile terminal to allow the transfer of IP data across the system of Figure 1.

Detailed Description of a Preferred Embodiment

30 Figure 1 illustrates a typical communications system in which a corporate intranet 1 is connected via a gateway (or "firewall") 2 to the Internet 3. A remote mobile terminal 4 such as a PDA with a cellular telephone "modem" may connect to the security gateway

2 via the Internet 3 and a Public Land Mobile Network (PLMN) 5. In the following discussion, it is assumed that the PLMN is a GSM network. By using IPSec to control communications between the security gateway 2 and the mobile terminal 4 (and hence between the mobile terminal 4 and local hosts 6 connected to the intranet 1), a Virtual
5 Private Network (VPN) may be established.

Figure 2 illustrates schematically the entities involved when a mobile terminal 4 requires authorisation to enter through a corporate intranet gateway 2. The sequence of events leading to a successful and secure connection is shown in Figures 3a and 3b and
10 is as follows:

1. The GSM mobile terminal 4 and Subscriber Identity Module (SIM) card to be inserted into the terminal are manufactured as normal. The SIM card includes a unique identifier such as an International Mobile Subscriber Identity (IMSI) or telephone
15 number. Additional information may be stored in the SIM card, depending on how the authentication is to be performed.

Upon each attempt by the mobile terminal 4 to enter through the intranet gateway 2, the following steps take place:

20

2. The terminal 4 initiates an IKE negotiation with the intranet gateway 2. This attempt is observed by the operator's security gateway 8 which routes all traffic from mobile terminals. Rather than allowing the IKE communication from the mobile terminal 4 to continue, the gateway 8 determines that the negotiations should be handled
25 by itself. This decision is communicated to the mobile terminal 4. It will be appreciated that for terminals which do not have this added value service enabled, the gateway 8 will remain transparent to IKE negotiations.

In an alternative system, it is possible for the mobile terminal 4 to contact the operator
30 gateway 8, rather than attempting to open IKE negotiations directly with the intranet gateway 2. The address of the operator gateway 8 could be included on the SIM card at step 2 above, or the terminal 4 could be configured by the user. However, the

interception of a direct IKE negotiation attempt is the preferred alternative because it requires no prior configuration of the terminal 4.

3. The terminal 4 runs GSM SIM-based authentication of IKE phase 1 with the operator's security gateway 8 according to the IETF draft proposal of Rinnemaa. This procedure identifies and authenticates the terminal 4 to the gateway 8 by reference to the Home Location Register (HLR) 9 of the network. Identification of the mobile terminal 4 is by way of the subscriber's IMSI or telephone number.

4. The operator's security gateway 8 authenticates itself to the terminal 4, to protect against rogue gateways. This can be performed using one of the following methods:

A shared secret authentication takes place using a secret previously agreed between the terminal 4 and the operator gateway 8. The secret could be stored on the SIM card of the terminal 4 (see step 2 above).

The terminal 4 is configured with the public key of the gateway 8 or of the CA 10 of all gateways (this could performed in step 2 above).

Step 4 completes the IKE phase 1 process between the mobile terminal 4 and the security gateway 8.

5. The operator's security gateway 8 determines the IP address of the corporate intranet gateway 2 from the destination address of the original IKE negotiation request made by the mobile terminal 4.

If the terminal 4 did not attempt a direct IKE negotiation with the corporate intranet gateway 2 as described in step 3 above, but initiated the request by contacting the operator's security gateway 8, then it will be necessary for the operator gateway 8 to determine the address of the corporate intranet gateway 2 by some other means. This may be, for example, by the use of pre-configured information in the operator gateway 8. Alternatively, the mobile terminal 4 could supply this information as part of the original request. The address of the corporate gateway 2 could be stored on the SIM

card at step 2 above, or as part of the user configuration of the terminal 4, and forwarded to the operator gateway 8.

6. The security gateway 8 identifies a certificate for the mobile terminal 4 by mapping the terminal's identity (e.g. IMSI) to a database of certificates. These certificates have previously been obtained by the gateway 8 as a result of negotiations with a CA. Each certificate contains a public key for the terminal as well as the identity, i.e. telephone number, of the terminal. The certificate is "signed" by encryption with the private key of a private-public key pair belonging to the issuing CA.

10 In some cases, the operator may itself act as a CA, in which case certificates may be generated by the operator (this could be done dynamically upon request by a subscriber).

7. The operator's security gateway 8 starts an IPsec/IKE Phase 1 negotiation with the corporate intranet gateway 2 using the identified certificate. This step (and steps 5 and 6) may occur simultaneously with step 3 above. The intranet gateway 2 knows the public key of the CA. The gateway 2 can therefore identify and authenticate the mobile terminal 4. The gateway 2 then proceeds to perform an authorization decision by, for example, checking the phone number of the mobile terminal against a list of allowed users. This list of allowed users is maintained in a local database (LDAP) 7.

15 20

In an alternative procedure, the operator 8 and the corporation maintaining the intranet gateway 2 have previously agreed the use of a special set of keys and CA parameters, effectively outsourcing normal PKI operations of the corporation 2 to the operator 8.

25 Standard IKE mechanisms will then be used, the only required checks being the key checks and the verification that the certificate comes from the corporation's own CA (operated by the operator). No LDAP is required.

8. The operator gateway must then authenticate the corporate gateway, by either:

30 using a pre-shared secret (i.e. shared between the terminal and the corporate gateway) or a public key stored in Step 1 at the terminal and later transported to the operator's gateway using a new IKE data element; or

using a pre-shared secret or a public key agreed with the operator and the corporation beforehand (the preferred alternative).

Step 8 concludes the IKE Phase 1 process between the security gateway 8 and the corporate intranet gateway 2.

At the end of IKE Phase 1, the two communicating nodes have authenticated each other and have established a shared secret. In IKE phase 2, the communicating nodes proceed to establish a pair of Security Associations (SAs). It is envisaged that IKE Phase 2 proceeds separately for both the mobile terminal to security gateway connection and for the security gateway to corporate gateway connection. Once the two pairs of SAs have been established, data can be carried securely between the mobile terminal 4 and the intranet gateway 2 with the security gateway performing any required translation. Alternatively, further SAs can be negotiated using the initial SA pairs.

In order to reduce the processing load on the security gateway 8, SA proposals (such as the encryption algorithm to be used) negotiated for one leg of the connection may be sent forward across the second leg. For example, SA proposals for the mobile terminal 4 to security gateway 8 connection may be forwarded to the intranet gateway 2. In this way, the same SA proposals may be used for both connection legs avoiding the need for any translation (e.g. between encryption algorithms). It may also be possible to carry out only a single IKE Phase 2 negotiation for the end to end connection between the mobile terminal 4 and the intranet gateway 2, avoiding the need for a separate Phase 2 negotiation for each connection leg.

It will be appreciated by the person of skill in the art that various modifications may be made to the embodiment described above without departing from the scope of the invention. For example, rather than conduct a new pair of IKE phase 1 procedures each time the mobile terminal seeks to access through the intranet gateway, the procedure may only be carried out the first time that such an access is sought, and regular time intervals thereafter (e.g. at 24 hour intervals). In another modification, the certificate identified by the security gateway may have a structure different from that described above. For example, the certificate may contain the mobile terminal ID and public key

in unencrypted form. A hash function is applied to the ID and public key, and the result encrypted with the CA's private key to generate a signature.

CLAIMS:

1. A method of authenticating a mobile wireless terminal to a correspondent node for the purpose of establishing an IP connection between the terminal and the node, the
5 method comprising:
 - authenticating and identifying the mobile terminal to a gateway node of a mobile telecommunications network;
 - at the gateway node, obtaining a certificate for the mobile terminal, which certificate can be used to identify and authenticate the mobile terminal;
 - 10 sending the certificate from the gateway node to the correspondent node; and
 - at the correspondent node, using the received certificate to identify and authenticate the mobile terminal.
2. A method according to claim 1, wherein the gateway node is an operator-owned
15 security gateway, and the operator gateway determines a public-private key pair on behalf of the mobile terminal, together with the certificate for the mobile terminal based on a mapping of a unique identifier of the terminal.
3. A method according to claim 1 or 2, wherein the certificate identified by the
20 gateway is a public key certificate obtained from a certification authority (CA).
4. A method according to claim 3, wherein said certificate contains an identification of the mobile terminal.
- 25 5. A method according to claim 4, wherein said identification is a phone number of the mobile terminal.
6. A method according to claim 4 or 5, wherein the correspondent node determines whether or not to authorise access to the mobile terminal on the basis of said identifier.
30
7. A method according to any one of the preceding claims, wherein said steps of sending the certificate from the gateway node to the correspondent node and of using

the received certificate to identify and authenticate the mobile terminal both form part of an IKE Phase 1 procedure.

8. A method according to any one of the preceding claims, wherein the step of authenticating the mobile terminal to the gateway node forms part of an IKE Phase 1 procedure which makes use of a SIM authentication procedure using the subscriber's IMSI.

9. A method according to any one of the preceding claims, wherein, when the mobile terminal attempts to perform IKE with the correspondent node, this attempt is recognised by the operator gateway, causing the operator gateway to authenticate the mobile terminal to the correspondent node and handle IKE negotiations with the correspondent node on behalf of the mobile terminal.

10. A method according to any one of claims 1 to 8, wherein the mobile terminal contacts the operator directly to cause the operator to open IKE negotiations with the correspondent node.

11. A method according to any one of the preceding claims, wherein the mobile wireless terminal is a cellular telephone or communicator, or a PDA, laptop computer, palmtop computer etc, having cellular telephone capabilities.

12. A method of establishing a secure connection between a mobile wireless terminal and a correspondent node, the method comprising the steps of:

authenticating the mobile wireless terminal to the correspondent node using the method of any one of the preceding claims; and

authenticating the correspondent node to said gateway node of the mobile telecommunications network.

13. A method according to claim 12 and comprising conducting an IKE phase 2 negotiation between the mobile wireless terminal and the correspondent node to establish one or more IPSec SAs.

14. A gateway node of a mobile telecommunications network, the gateway node comprising:

means for authenticating and identifying a mobile wireless terminal;

5 means for obtaining a certificate for the mobile terminal, which certificate can be used to identify and authenticate the mobile terminal; and

means for sending the certificate from the gateway node to the correspondent node,

wherein the received certificate may be used by the correspondent node to identify and authenticate the mobile terminal for the purpose of establishing an IP
10 connection between the terminal and the node.



INVESTOR IN PEOPLE

Application No: GB 0028618.7
Claims searched: 1-14

Examiner: Robert Shorthouse
Date of search: 9 August 2001

Patents Act 1977 Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.S): H4L (LRCMS, LRCMA, LDPD, LDPPX), H4P (PDCSA)

Int Cl (Ed.7): H04Q 7/38, H04L 9/32, 29/06

Other: Online: WPI, EPODOC, JAPIO, INSPEC

Documents considered to be relevant:

Category	Identity of document and relevant passage	Relevant to claims
A	GB 2342817 A (NOKIA) See abstract	-
A	WO 00/02406 A2 (NOKIA) See abstract	-
A, P	WO 01/17310 A1 (ERICSSON) See abstract	-

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.